

5. Cracking Passwords

Crack the extracted password hashes

- Use John the Ripper or Hashcat to crack the password hashes.

```
hashcat64 -m 1000 -a 0 hashes.txt rockyou.txt
```

- `-m 1000`: This specifies that the hash type is NTLM (for Windows hashes).
- `-a 0`: This specifies a dictionary attack.
- `<wordlist>`: Replace this with the path to your wordlist file (e.g., `rockyou.txt`).

```
16a746500673b41d9a4dd37994a3a835:cantona  
3aebfe39627c56e3ec440c9f432f73f3:whiterose
```